UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,682	01/23/2004	Brant L. Candelore	80398P252X3	9474

8791 7590 05/04/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
BAYOU, YONAS A	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
05/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/764,682	CANDELORE, BRANT L.	
	Examiner	Art Unit	
	Yonas Bayou	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :09/27/2004/, 09/29/2004, 01/03/2005, 07/21/2006, 12/11/2006.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: "a receiver ill" should be "a receiver 111" **[page 2, paragraph 0039].**

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1- 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Wasilewski US Patent No. 6,157,719.

Referring to claims 1, 3, 12 and 13, Wasilewski teaches a mating key gateway adapted to retrieve at least one mating key used to encrypt a program key that is used to scramble digital content prior to transmission to a digital device, comprising:

a bus **[column 14, lines 14-16** a bus is inherently a communication scheme (wires, fiber optics, fiber coax)];

a processor coupled to the bus **[column 21, lines 15-19 and fig. 12];**

an interface coupled to the bus, the interface being adapted to receive information from (1) a sender of the digital content and (2) either a server controlled by a supplier of the digital device or a trusted third party **[column 21, lines 15-21; fig. 12;** interface 1203 (equivalent to an interface) connected to a bus permits passage of data between the components of DHCT 333 and DHCTSE 627 which is inherently the interface coupled to the bus, being adapted to receive information from a sender/a headend];and

a non-volatile storage unit coupled to the bus, the non-volatile storage unit to store a mating key lookup table to identify either the server controlled by the supplier of the digital device or the trusted third party based on the information received from the sender **[column 21, lines 9-22; fig.13;** NVA storage 1303 stores administrative storage (keys) which contains DHCT keys 1325 each DHCT 333 has public-private key pair to encrypt EMMs sent to DHCT 333 and to decrypt the messages respectively, i.e. to secure the information received from the sender/the headend which is inherently store a mating key to identify the server controlled by the supplier of the digital device].

Referring to claim 2, Wasilewski teaches the mating key gateway, wherein the interface to receive the information from the sender being one of a cable provider, a satellite-based provider, a terrestrial-based provider, an Internet service provider and a

conditional access (CA) provider operating with one of the cable provider, the satellite-based provider, the terrestrial-based provider and the Internet service provider **[column 10, lines 52-55; column 13, line 64 - column 14, line 8**; DHCT 333 (interface to DHCT) receive the information from the provider, i.e., conditional access (CA) provider, cable provider, internet service and etc].

Referring to claims 4 and 14 Wasilewski teaches the mating key gateway, wherein the information received by the interface from the sender comprises a mating key generator being a message that comprises an identifier of the supplier **[column 18, lines 1-15**; the sender/headend comprises a mating key generator (equivalent to a type of message/key generator, i.e. ECM, EMM, GBEM and etc.) being a message that contains an identifier of the conditional access system which inherently the supplier].

Referring to claims 5 and 25, Wasilewski teaches the mating key gateway inherently the security content delivery system, wherein the mating key generator received by the interface further comprises an identifier of a provider of a system that enables transmission of both the digital content and the mating key generator to the digital device **[column 17, line 59-column 18, line 15; column 24, lines 21-26; column 29, lines 44-47;** an identifier of CAA (conditional access authority) which is a part of the trusted third party is inherently an identifier of a provider and do security checking to the program (content) over transmission so that it enables execution].

Referring to claims 6, 15 and 26, Wasilewski teaches the mating key gateway, wherein the mating key generator received by the interface further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the digital content and the mating key generator are transmitted, and (ii) a mating key sequence number **[column 19, lines 55-65; fig. 10 and column 24, lines 21-34**; an identifier for the CAA or EA is inherently an identifier of a provider helps to secure and transmit data; and the mating key generator (equivalent to CA message 805 in fig. 11) includes a sequence of CA message which is inherently a mating key sequence number].

Referring to claims 7, 16 and 17, Wasilewski teaches the mating key gateway, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of serial numbers for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of suppliers **[column 7, lines 5-8 and fig. 2B**; DHCT (equivalent to digital device) has serial number stored in memory supplied by supplier/manufacturer); **column 33, lines 54-60; column 43, lines 55-65**; EAID (entitlement agent ID) inherently is the information to communicate with a server].

Referring to claims 8, 10 and 19, Wasilewski teaches the mating key gateway, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i)

a first group of entries forming a range of serial numbers for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including an address to establish communications with a trusted third party authorized by one of the plurality of suppliers **[column 7, lines 5-8; fig. 2B; column 16, lines 47-49; column 22, lines 23-35; column 33, lines 22-60; column 47, lines 4-33 and fig. 28**; an address to the EA/DHCT 333'S private key matches with DHCT 333's true key which is accomplished by certifying the DHCT certificate 2806 with the factory programmer certificate authority (FPCA)/(equivalent to control suite 607 in fig.6) which inherently a trusted third party signature to establish a secured communications over a network 521 (fig. 6)].

Referring to claims 9, 11 and 18, Wasilewski teaches the mating key gateway, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of mating key generators for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of suppliers **[column 7, lines 5-8 and fig. 2B**; DHCT/digital device (equivalent to mating key generator) comprises key/mating key corresponding to one of the mating key generator stored in memory which is supplied by each supplier/manufacturer; **column 33, lines 54-60; column 43, lines 55-65**;

EAID (entitlement agent ID) inherently is the information to communicate with a server].

Referring to claim 20, Wasilewski teaches the mating key gateway being adapted to additionally store mating keys for selected digital devices **[column 4, lines 41-63 and fig. 1**; set-top box 113 (equivalent to mating key gateway) additionally store mating keys/information].

Referring to claim 21, Wasilewski teaches a secure content delivery system comprising:

a trusted third party to store a plurality of mating keys associated with digital devices, each mating key being used to encrypt a key that is used to scramble digital content **[column 22, lines 23-35; fig. 6**; a control suite 607 (equivalent to a trusted third party) stores keys/mating keys which inherently used to encrypt digital content];

a mating key gateway in communications with the trusted third party, the mating key gateway to provide information received from a head end to the trusted third party for retrieval of a requested mating key **[column 15, lines 7-23; column 16, lines 47-55 and fig. 6**; the communications between the trusted third party/control suite 607 and the rest of conditional access system 601 (includes a key generator/a mating key gateway) is to make ECM and EMM which is inherently for retrieval of a requested mating key].

Referring to claim 22, Wasilewski teaches a secure content delivery system, wherein the key used to scramble the digital content is a program key **[column**

5, lines 26-28].

Referring to claims 23 and 24, Wasilewski teaches a secure content delivery system, wherein the information provided to the trusted third party comprises a mating key generator being a message that comprises an identifier of a supplier of one of the digital devices **[column 18, lines 4-15**; the information provided to ECM/EMM (part of the trusted third party) which inherently contains a key generator and ID of a supplier].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 27, 28, 30 and 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski US Patent No. 6,157,719 in view of Turner et al. US Patent No. 6,707,696.

6. Referring to claim 27, Wasilewski teaches a step of receiving a mating key generator; and outputting a mating key based on the mating key generator **[column 7, lines 5-8 and fig. 2B]**. Wasilewski fails to teach a one-time programmable value being

identical to a key stored in a digital device of a set-top box targeted to receive information encrypted with either the mating key or a derivative of the mating key. However, Turner teaches a one-time programmable value being identical to a key stored in a digital device of a set-top box targeted to receive information encrypted with either the mating key or a derivative of the mating key; **[column 1, lines 30-37; fig. 3**; TV Decoder Box (equivalent to set-top box) has a SRAM 306 (equivalent to a mating key generator) and one-time programmable memory, both holds encryption keys that are compared by the processor 305 which is inherently outputting a mating key based on the mating key generator and an one-time programmable value being identical to a key stored in a set-top box targeted to receive information encrypted with either the mating key or a derivative of the mating key].

At the time of the invention was made, it would have been obvious to a person of ordinary skill in the art to use Turner's hacker-proof one-time programmable memory with Wasilewski's Conditional access system because it offers the advantage of having a mating key and an one-time programmable value to receive information encrypted with either the mating key or a derivative of the mating key.

Referring to claim 28, Wasilewski teaches the step of outputting the mating key **[column 1, lines 30-37; fig. 3 and column 14, lines 14-16]**. Wasilewski fails to teach receiving a serial number being used to locate the one-time programmable value. However, Turner teaches receiving a serial number being used to locate the one-time

programmable value **[column 2, lines 1-10; fig. 7**; an address decoder communicates with the power up write controller and the read controller, for providing an address to the one-time programmable memory array which is inherently the method receives a serial number being used to locate the one-time programmable value].

At the time of the invention was made, it would have been obvious to a person of ordinary skill in the art to use Turner's hacker-proof one-time programmable memory with Wasilewski's Conditional access system because it offers the advantage of receiving a serial number being used to locate the one-time programmable value prior to outputting the mating key.

Referring to claim 30, Wasilewski teaches a secure content delivery System/method, wherein the mating key generator includes at least one of (i) a first identifier to identify a manufacturer of the digital device **[column 18, lines 4-15],** (ii) a service provider identifier **[column 17, line 59-column 18, line 15; column 24, lines 21-26,** (iii) a conditional access provider identifier, and (iv) a mating key sequence number **[column 19, lines 55-65; fig. 10 and column 24, lines 21-34]**.

Referring to claim 32, Wasilewski fails to teach a conditional access (CA) control system in communication with a mating key server, the CA control system comprising: means for receiving a mating key from the mating key server, the mating key being computed based on a mating key generator and a one-time programmable value; and

means for producing a plurality of derivatives keys based on the mating key, each derivative key being used to encrypt a key that is configured to descramble digital content targeted for a digital device of a set-top box. However, Turner teaches a conditional access (CA) control system in communication with a mating key server, the CA control system comprising: means for receiving a mating key from the mating key server, the mating key being computed based on a mating key generator and a one-time programmable value; and means for producing a plurality of derivatives keys based on the mating key, each derivative key being used to encrypt a key that is configured to descramble digital content targeted for a digital device of a set-top box **[column 3, lines 25-39; column 3, lines 47-50; fig. 3 and fig. 7;** Power-Up Write Controller (equivalent to conditional access (CA) control system) communicates inherently with the service provider/server and keys from TV Decoder Box 301].

At the time of the invention was made, it would have been obvious to a person of ordinary skill in the art to use Turner's hacker-proof one-time programmable memory with Wasilewski's Conditional access system because it offers the advantage of receiving a mating key from the mating key server, the mating key being computed based on a mating key generator and a one-time programmable value; and means for producing a plurality of derivatives keys based on the mating key, each derivative key being used to encrypt a key that is configured to descramble digital content targeted for a digital device of a set-top box.

Referring to claim 33, Wasilewski teaches a secure content delivery

system, wherein the key used to scramble the digital content is a program key **[column 5, lines 26-28].**

Referring to claim 34, Wasilewski teaches the CA control system comprising: transmitting the encrypted program key and the scrambled digital content to the digital device of the set-top box **[column 6, lines 18-23].**

7. Claims 29 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski US Patent No. 6,157,719 in view of Turner as applied to claim 27 above, and further in view of Smeets et al. US Patent No. 7,058,806. The teaching of Wasilewski in view of Turner has been discussed above.

Referring to Claims 29 and 31, Wasilewski teaches the step of outputting the mating key **[column 1, lines 30-37; fig. 3 and column 14, lines 14-16].** Wasilewski in view of Turner fails to teach computing the mating key by performing a computation on the mating key generator and the one-time programmable value to produce a mating key. However, Smeets teaches computing the mating key by performing a computation on the mating key generator and the one-time programmable value to produce a mating key **[column 8, lines 18-31; fig. 4; fig. 3; column 9, lines 12-20 and fig. 6**; computing between system 600 (equivalent to one-time programmable value) and external device 670 (equivalent to the mating key generator) to produce authentication key (equivalent to a mating key)].

At the time of the invention was made, it would have been obvious to a person of ordinary skill in the art to use Smeets's method and apparatus for secure leveled access control with Conditional access system as taught by Wasilewski in view of Turner because it offers the advantage of computing the mating key by performing a computation on the mating key generator and the one-time programmable value to produce a mating key.

8. Claims 35-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski US Patent No. 6,157,719 in view of Smeets et al. US Patent No. 7,058,806.

Referring to Claim 35, Wasilewski teaches a method receiving a request for a key over a communication bus **[column 7, lines 5-8 and fig. 2B]**. Wasilewski fails to teaches a method recovering different versions of the key depending on which of a plurality of providers is requesting the key; and providing the different versions of the key to the plurality of providers adapted to use the key as either a mating key to encrypt digital content delivered to a targeted digital device or as a precursor key to derive the mating key to encrypt the digital content delivered to the targeted digital device. However, Smeets teaches a method recovering different versions of the key depending on which of a plurality of providers is requesting the key; and providing the different versions of the key to the plurality of providers adapted to use the key as either a mating key to encrypt digital content delivered to a targeted digital device or as a precursor key to derive the mating key to encrypt the digital content delivered to the

targeted digital device **[column 5, lines 14-28; fig. 2].**

At the time of the invention was made, it would have been obvious to a person of ordinary skill in the art to use Smeets's method and apparatus for secure leveled access control with Wasilewski's Conditional access system because it offers the advantage of receiving a request for a key over a communication bus; recovering different versions of the key depending on which of a plurality of providers is requesting the key; and providing the different versions of the key to the plurality of providers adapted to use the key as either a mating key to encrypt digital content delivered to a targeted digital device or as a precursor key to derive the mating key to encrypt the digital content delivered to the targeted digital device.

Referring to Claim 36, Wasilewski fails to teach the method recovering of the key includes accessing a database to retrieve the key being a pre-calculated value. However, Smeets teaches recovering of the key includes accessing a database to retrieve the key being a pre-calculated value **[column 4, lines 29-38; fig. 1;** which inherently retrieve the key being a pre-calculated value].

At the time of the invention was made, it would have been obvious to a person of ordinary skill in the art to use Smeets's method and apparatus for secure leveled access control with Wasilewski's Conditional access system because it offers the advantage of recovering of the key includes accessing a database to retrieve the key being a pre-calculated value.

Referring to Claim 37, Wasilewski fails to teach the method recovering the key

includes calculating the key substantially in real time based on a unique key associated with the targeted digital device, an identical copy of the unique key being permanently stored within the targeted digital device. However, Smeets teaches the method recovering the key includes calculating the key substantially in real time based on a unique key associated with the targeted digital device, an identical copy of the unique key being permanently stored within the targeted digital device [column 4, lines 4-14; fig. 1].

At the time of the invention was made, it would have been obvious to a person of ordinary skill in the art to use Smeets's method and apparatus for secure leveled access control with Wasilewski's Conditional access system because it offers the advantage of recovering the key includes calculating the key substantially in real time based on a unique key associated with the targeted digital device, an identical copy of the unique key being permanently stored within the targeted digital device.

Referring to claim 38, Wasilewski teaches the mating key gateway inherently the security content delivery system, wherein the mating key generator received by the interface further comprises an identifier of a provider of a system that enables transmission of both the digital content and the mating key generator to the digital device **[column 17, line 59-column 18, line 15; column 24, lines 21-26; column 29, lines 44-47;** an identifier of CAA (conditional access authority) which is a part of the trusted third party is inherently an identifier of a provider and do security checking to the program (content) over transmission so that it enables execution].

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yonas Bayou whose telephone number is 571-272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Yonas Bayou

YB

KIMBERLY D. NGUYEN
PRIMARY EXAMINER